POSITION STATEMENT FROM BCS FOR W3C WORKSHOP PARIS 24-25 MARCH 2014 – "HOW DO YOU WANT TO PAY?" – LOUISE BENNETT

BCS VIEWS ON IDENTITY ASSURANCE AND PAYMENTS ON THE INTERNET

Over the last three years the Identity Assurance Working Group (IAWG) of BCS[1] – The Chartered Institute for IT – a UK based worldwide professional body for IT with over 80,000 members - has been examining the governance and other issues surrounding identity assurance on the Internet at the request of their membership.

The BCS position is that:

- Implications of W3C open standards for ID and payments and tensions between these and many different jurisdiction's views require resolution.
- Identity governance on the Internet is now a mainstream global issue that is central to trust in Internet transactions
- The Internet needs to remain a global commons and not become a gated commons, as some would wish, following the NSA surveillance leaks.
- Big data collection and analytics is increasingly being challenged, both from the perspective of national surveillance and security issues and from the perspective of commercial exploitation of customer/user data. It will be essential to both protect positive uses of personal data to help assert ID and make payments on the Internet and deter uses without consent that are not for societal or individual benefit.
- Personal Data is the currency of today's digital market, but individuals need to be educated about this so that they can keep control.
- The tensions and proportionality between: privacy/ intimacy and anonymity/ traceability require continued discussion. All are context sensitive and security is always needed.

1. INTRODUCTION AND BACKGROUND

In 2011 the OECD stated that digital identity management was at the core of the Internet economy[2]. A major development in 2013 has been that this view is now widely accepted. Identity governance is now considered a mainstream global issue applying, in particular, to payment transactions between individuals and organisations.

The BCS has traced the developing views of identity governance over the Internet from both UK and global perspectives. The views have been collected from attendance at meetings throughout 2011 - 13 by members of the BCS IAWG[3]. The Group aims to help drive the improvements that are needed globally on Identity Management and Assurance

[1] www.bcs.org

2 OECD (2011), "Digital Identity Management for Natural Persons: Enabling Innovation and Trust in the Internet Economy - Guidance for Government Policy Makers", *OECD Digital Economy Papers*, No. 186, OECD Publishing. http://dx.doi.org/10.1787/5kg1zqsm3pns-en

[3] The IAWG is a subgroup of the BCS Security Community of Expertise (SCoE) and is made up of members of the SCoE with invited experts from industry and academia.

over the Internet primarily through the UN Internet Governance Forum (UNIGF). The IAWG supports the UK Government view that the UNIGF multi-stakeholder approach to improving Internet Governance is the most effective way to make progress.

Each year BCS produces Aspects of Identity Yearbooks[4].

In 2011 the BCS started with a conventional set of key issues associated with electronic identities:

1. Citizen's rights and control of personal data
2. Minimising access and controlling privacy
3. Registration authorities and ID assurance
4. Rights and responsibilities of ID providers, and
5. The balancing act of security versus privacy

This covered the whole framework for identity governance on the Internet and the complex topic of trust in transactions with remote identities: anonymity, pseudo-anonymity and attribution.

In 2012 the focus shifted to several controversial topics identified in 2011:

1. The proportionality between security, privacy and anonymity
2. Identity discovery through data aggregation and data mining
3. The commercialisation of the Internet and monetisation of identity attributes
4. Legal and commercial frameworks for payments
5. How to use various attributes of identity for access to online resources

BCS still stands by its views on all these issues, which can be found in the Yearbooks. The key topics of identity assurance: how to ensure confidence in the people, organisations and things you are dealing with on the Internet, preventing identity theft and protecting the naive from themselves remain the overriding objectives of sound Internet identity governance.

In 2013 more workshops and seminars were held in UK, Europe and at the UNIGF. These focussed on:

1. The drivers for privacy and anonymity (accepting that security underpins both)
2. Basing identity in e-commerce on liability models and contractual frameworks
3. The positives and negatives of identity as currency on the Internet
4. The link between different motivations to go online and securing online identity in each context
5. How both national and global single purpose schemes, fit for different purposes, can interoperate (since we reject the notion of any single grand scheme).

2. INTERNET LANDSCAPE 2013-14

In 2013 the focus of global tensions moved into cyberspace. In the 1980s global tensions focussed on the cold war. After the Berlin Wall came down an era of detente was ushered in during the 1990s. After 9/11 the focus shifted to terrorism. In 2013 global tensions moved decisively to the cyber-sphere. Intelligence and data gathering in cyberspace was already the key topic in discussions between the two global superpowers, the USA and China, before the Snowdon revelations about NSA surveillance. Since then the steady drip, drip, drip of Snowdon's stolen information to the world's media has done much to erode

[4] Aspects of Identity Yearbook 2011-12 – BCS Identity Assurance Working Group 2012 – ePUB ISBN:978-1-78017-141-8, Aspects of Identity Yearbook 2012-13 – BCS Identity Assurance Working Group 2013 – ePUB ISBN:

trust between nations and cultures on the Internet. As trust is inextricably bound up with identity assurance, payments and issues of privacy, Snowdon has had a profound effect on Internet Identity Governance. It seems likely that nation states will no longer trust each other's standards/PKI/eID systems, and there may be a rise in independent, off-shored services which refuse to disclose their root keys to intelligence services.

Another issue that is now being widely debated is the question of identity discovery through personal data aggregation. Big Data collection, aggregation and analysis, particularly where parts of the data sets contain personally identifiable data is a major ethical issue. While it has been emotively dominated by NSA surveillance, it is a much broader issue than this. Snowdon is in danger of diverting everyone's attention away from what NGOs and commercial organisations are doing with Big Data and focussing attention solely on spying. The privacy issues surrounding data collection and analytics are enormous and require a rational, unemotional debate about when societal good outweighs personal privacy.

It is now widely acknowledged that information on the Internet is all discoverable by anyone determined to do so. Absolute privacy and anonymity online are chimeras, as they are in the physical world. However, people do need to have the means of ensuring security for their online identities that are commensurate with the contexts of different online interactions.

In connection with all the issues associated with online identity there is a growing need for widespread public education about safe use of the Internet. This is a key requirement for the Internet to flourish and to ensure that all nations, businesses and individuals get economic benefits from an increasingly online world.

In addition there are specific and particular needs for web payments that would be usefully underpinned by a set of worldwide open standards and associated security.

3. IDENTITY RELATED ISSUES FOR ON-LINE PAYMENTS

Major US Companies have now formed the Reform Government Surveillance Alliance to counter the anti-American feelings about the Internet and loss of business by those companies particularly in cloud computing. In the commercial context it is worth remembering that fragmentation is not a new worry; the internet as a unitary entity free and open to all has been under pressure from commerce for years. Many of the product sets and apps intended to differentiate major providers from each other have a side effect of creating "walled gardens" and weakening net neutrality. These "walled gardens" would be global, but provider specific, and the BCS position is that these should also be resisted.

Since there are now over 500,000 interlinked networks on the Internet, the practicality of separating these is near impossible. However, some countries are determined to build barriers and defend "great walls", insisting on their own governance behind and within them. Even if just political posturing, this is deeply counter-productive. This is particularly the case for massive online data storage and cloud computing. There may be two factors countering this, to BCS eyes, adverse trend. The first will depend on the effectiveness of the response of nation states, and the USA in particular, to the general outcry over the activities of the intelligence agencies which has culminated in the UN General Assembly unanimously adopting a resolution affirming the right to privacy in the digital age[5]. The second is the potential for the tension between the desires of the large commercial internet providers to make global profits (albeit within their own global "walled gardens") and the movement of some nations towards "balkanisation". This is obviously a very

[5] http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N13/576/77/PDF/N1357677.pdf?OpenElement

sensitive balance to achieve and maintain and BCS will continue to monitor the development of these trust related matters.

The WorldWide Web Consortium (W3C) is currently developing an infrastructure for web identity and payment standards (PaySwarm) that has the potential to be a major disruptive force that could encourage many new business models and enable the unbanked and digitally excluded to benefit from online services. It offers a decentralised ID, using a secure digital signature and Web Key encryption. It operates by creating an ID with the PaySwarm Authority, associating a Web Key with this ID, registering it with the PaySwarm Listing Service. The user then constructs a purchase request, signs it digitally and receives a receipt that contains the transaction ID and contract. This is a model that the BCS supports. It complements the existing worldwide banking models used for credit and debit card payments and has the potential to enhance the mobile phone payments models, such as M'pesa, which is widely used in East Africa.

A particular area of concern to BCS relates to payments using Near Field Communications (NFC) for on-line mobile payments. It is important that the standards for these are fully discussed as part of the W3C work and are fit for global payments.

The associated issues that need fuller discussions are jurisdictional issues related to disputes and liability models enabling redress. We need to recognise that trust and liability go together; you cannot have one without the other. Trust is based on the fact that if, even though it is unlikely, something goes wrong with a transaction, what recourse does one have, who can one look to for liability/redress, where does 'the buck stop'? What responsibilities are taken on by one party and what entitlements can be expected by the other party?

The default 'solution' is that 'government must step up to fill this void', but in virtually every nation-state discussion worldwide, it quickly becomes clear that government simply cannot undertake such a role; regardless of whether businesses or the citizen 'trusts' their government. Government in itself is not equipped either to take on the liabilities or to accept the obligations associated with vouching for the eidentity of the citizens/businesses falling within its geographic confines.

So, if not government, who then can step up to provide such a blend of trust and liability, and who can manage the associated risks in a 'joined up' manner around the world? Who can do so in such a way that governments can be happy that such entities are regulated/can be overseen?

The answer lies in considering what works today and how it works. Take the worldwide 'payments industry' as the nearest illustration of an 'application' that is both local and global, that crosses all sectors, and that moves (increasingly) in a near instantaneous manner. Consider a payment (such as a credit card payment) as being essentially the movement of bits and bytes of digital information representing (money) value, from one digital identity (namely a bank account) to another digital identity (another bank account) via other trusted digital identities (credit card schemes). We take this largely for granted in our daily lives, we trust it, but we do so substantially because we know that, if anything goes wrong, then there is a pre-established route of recourse usually backed by national legislation. Therefore it does not matter if we buy something on holiday or buy something from another country over the internet, if something goes wrong, national legislation provides protection and recourse.

Almost all steps in commerce (public or private sector) in the internet era require exactly such a capability: the ability for some form of trusted/regulated intermediaries to work together under a common set of pre-agreed terms and conditions spanning both local and global geographies and industry sectors, public or private sector, to underpin the digital identity of each party.

4. CONCLUSIONS

To make progress on internet identity governance and associated payments it is essential that a true multi-stakeholder approach is adopted. This is difficult because it is not possible to make various obvious stakeholders attend a forum such as the UN IGF. Nevertheless, it is essential to pursue involvement of players from all aspects of at least two dimensions. The first dimension is the cultural and, in particular, different cultures' understanding and reaction to privacy. By this we do not mean at the broad level such as Asian, Western European etc. but a more nuanced approach to the problem The second important dimension (which will interact with the first) is sectoral (e.g. civil society, academia, commerce, industry, government, judiciary, etc.). The way forward is to ensure that BCS builds on its relationships with all of these stakeholders and ensures that a defensible position is developed and maintained.

When BCS talked with W3C about the new open standards that they are developing at the UNIGF, their greatest concern seemed to be the difficulty in engaging with legislators and regulators. In our opinion UK and EU legislators should engage with this initiative to ensure it fits in with acceptable regulatory regimes embraced in the London financial centre and elsewhere in the world. To this end BCS has made and will continue to make recommendations to the UK Parliament and Internet Conference in late 2013 and to UK representatives in the EU parliament on the subject of Internet payments.